SCOTTS INTERNATIONAL

Industrial Control Systems (ICS) Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 110 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Industrial Control Systems Security Market size is estimated at USD 13.52 billion in 2024, and is expected to reach USD 19.86 billion by 2029, growing at a CAGR of 8% during the forecast period (2024-2029).

Key Highlights
-The transition to Industry 4.0 is expected to bring many advances in efficiency and productivity, as well as many changes in the way the industrial processes work. Compared to the conventional manufacturing process, improved efficiency and reduction in production costs have boosted the adoption of automation, driving the demand for industrial control systems. However, the adoption of ICS solutions brings along the need for security, as there is an exponential rise in cyber-attacks and network security threats.
-The growing number of cyber threats has fueled revenue growth in the worldwide industrial control systems security market. With the increasing number of cyber-attacks, the adoption of industrial control systems is increasing in the manufacturing, chemical, energy, and other industries. With increasing attempts by hackers to enter business networks, the use of ICS security is growing significantly. Furthermore, the adoption of advanced technologies is resulting in the generation of massive amounts of data, increasing demand for ICS security, and as a result, driving revenue growth in the global market.
-The stringent government rules and regulations related to the Continuous Improvement Programme (CIP) to increase the adoption of ICS security solutions and the adoption of advanced technologies such as the Internet of Things (IoT) in industries has increased demand for the ICS security market. The industrial network infrastructure's large number of connected sensors and controllers has made security more difficult. The growing use of IoT technology and other network devices in industries has expanded the threat surface for criminals. ICS security is necessary for organizations' IoT applications, which will drive the market.
-The COVID-19 pandemic and lockdown restrictions across the region have affected industrial activities. The pandemic increased consumers' dependence on the internet, further increasing the market for industrial control systems. The outbreak of COVID-19

has forced manufacturing industries to re-evaluate their traditional production processes, primarily driving the digital transformation and smart manufacturing practices across the production lines. The manufacturers are also forced to devise and implement multiple new and agile approaches to monitor product and quality control.
-The aging hardware or software of the ICS in many organizations is another factor responsible for increased complexity. Most organizations still use legacy ICS, owing to their importance in the functioning of the plant. This increased age of ICS leaves ample opportunities for cyberattacks and increases complexity. Also, the cost of a security system or platform is another factor hindering the deployment of ICS security services in organizations. Justifying the cost incurred for the security solutions is quite difficult for various reasons.

Industrial Control Systems Security Market Trends

Automotive is Expected to Hold a Significant Share

- ICS offers opportunities to the automotive industry to react faster to the market requirements, reduces manufacturing downtimes, enhances the efficiency of supply chains, and expands productivity.
- Field devices, such as robotics and sensors, and ICS offer opportunities to the auto sector to react faster to market requirements, reduce manufacturing downtimes, enhance efficiency, and expand productivity.
- The automotive industry is among the prominent sectors that hold a significant share of automated manufacturing facilities worldwide. The production facilities of various automakers are automated to maintain efficiency. The rising trend of replacing conventional vehicles with electric vehicles (EVs) is expected to augment the automotive industry's demand further. For instance, IEA states global electric car sales doubled from 3.0 million in 2020 to 6.6 million in 2021.
- Various automotive enterprises are forming partnerships with the ICS providers to upgrade their facilities. For example, S&T Technologies, a provider of IoT software framework, SUSiEtec, and ICONICS signed a collaboration agreement. The contract specifies that S&T Technologies will integrate SCADA capabilities into the SUSiEtec software framework.
- Despite a considerable slowdown in the automotive industry, automotive production facilities led by electric vehicle manufacturers are expected to increase the number of smart/internet-connected ICS solutions installed in a facility, significantly increasing the demand for ICS Security solutions.

North America is Expected to Hold the Largest Share

- North America has been a pioneer in implementing ICS security solutions. This region has also been extremely responsive to the latest technological advancements, such as integrating cloud and IoT with ICS security solutions to set a holistic secure access mechanism and enforce a security governance framework. The Public-Private Partnerships and international partnerships have led to effective ICS security and resilience in the region.
- According to the Department of Homeland Security (DHS), The private sector owns 85% of critical infrastructure in the United States, including oil and gas, banking and finance, transportation, utilities, electric power grids, and defense. In contrast, the public sector regulates the rest. For instance, the region's energy and power grid sectors require public, private, and regulatory collaboration among DHS, the Department of Energy (DOE), and the Department of Defense (DOD) to protect their operational technology and Industrial Control Systems from cyber threats. Furthermore, cloud-based ICS security solutions and services are becoming increasingly popular in this region.
- Canadian manufacturers rely on innovation and investment in technologies to be competitive. The increasing input, labor cost, and competition from large global manufacturers enabled the country to invest in ICS and allied technologies to remain competitive and maintain its operating margins.

- Furthermore, according to the Government of Canada 2021, the manufacturing industry is estimated to contribute more than 10% to the Canadian GDP. The manufacturing sector is the largest investor in the R&D and implementation of new technologies in Canada.
- Recently, MITRE Corporation released ATT&CK for Industrial Control Systems, a taxonomy of cyber attack behavior targeting ICS. The company was launched to address critical infrastructure operations in manufacturing and utility industries with financial and espionage-motivated attacks and industry awareness.
- However, the country's resistance to regulation and growing complexities in securing ICS systems may act as a roadblock to the passage of critical infrastructure cybersecurity legislation.

Industrial Control Systems Security Industry Overview

The Industrial Control System Security Market is highly competitive and consists of several major players. Many companies have been increasing their market presence by introducing new products, entering partnerships, or acquiring companies.

- September 2021 - Honeywell acquired privately held Performix Inc., a manufacturing execution system (MES) software provider for the pharmaceutical manufacturing and biotech industries. The acquisition builds on Honeywell's strategy to create the world's leading integrated software platform for customers in the life sciences industry, striving to achieve faster compliance, improved reliability, and better production throughput at the highest levels of quality.
- August 2021 - CyberProof, a leading provider of cyber security solutions based in California, United States., announced a collaboration with Radiflow, a Tel Aviv-Yafo, Israel-based provider of cyber security solutions for industrial networks. In addition, the partnership strengthens CyberProof's ability to provide comprehensive Managed Detection and Response (MDR) services for converged Information Technology (IT) or Operational Technology (OT) systems.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Scotts International. EU Vat number: PL 6772247784
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com

SCOTTS INTERNATIONAL

Industrial Control Systems (ICS) Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 110 pages | Mordor Intelligence

To place an Order with Scotts International:
- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-04
		Signature	